Failure Detection | Silent Failure | All-IP Network

Technology Reports

Special Articles on All-IP Network Technology —Evolution of Core Network —

Highly Accurate Failure Detection System for Large-scale IP Networks

In recent years, various techniques for maintaining IP network security and reliability have been studied. One product of that work is a system that can rapidly and accurately detect silent failures in an IP network and determine of the failure location. That capability can prevent large-scale service failures due to silent failures and thus allow provision of high quality of service to users. This work was conducted jointly with Fujitsu, Ltd.

Core Network Development Department
Hironobu Kono
Yutaka Miyawaki
Network Management Division
DOCOMO Technology, Inc.
Taisei Kato
Minoru Ikeda

1. Introduction

In recent years, progress in network technology has increased the widespread use of broadband network access, and various IP services are being offered, such as IP telephony and e-mail. The IP network is also growing in social importance as the telecommunication infrastructure that supports such services.

As network scale increases, failures become more evident and their social effects magnify. A study on "Issues in the Operation of Large-scale IP Networks" is being conducted under guidance of the Ministry of Internal Affairs and Communications (Information and Communications Council). In that study, "research and development of IP network facility monitoring technology such as functions for early problem detection and autonomous switching to back-up equipment" and "faster identification of failure location and cause" [1] [2] are proceeding as particularly important measures for maintaining security and reliability in large-scale IP networks. One issue that has been identified for study is the detection of silent failures and determining where the failure occurred (hereinafter referred to as "failure location").

Detection of telecommunication equipment failures in an IP network generally uses the Telecommunication Network (TELNET)[*1], Simple Network Management Protocol (SNMP)[*2] or SYSLOG[*3] protocol. The results of messages sent from the monitored telecommunication equipment and periodic requests for device status sent to the relevant devices are collected and displayed. Maintenance personnel use that information for failure analysis and recovery. However, when failures due to bugs in the telecommunication equipment or failure in the detection

*1 **TELNET**: Virtual terminal software that allows operation of a remote server from a local computer over a TCP/IP network, or a protocol that makes such operation possible.
*2 **SNMP**: A protocol for the monitoring and control of communication devices (router or computer, terminals, etc.) on a TCP/IP network.
*3 **SYSLOG**: A protocol for recording system operation conditions and error messages and exchanging the data with other computers via a network.

unit or main processor occur, the telecommunication equipment itself is unaware of the failure. Therefore, no alarm is issued and the monitoring system cannot detect the failure. Such failures are called a silent failures (**Figure 1**). This type of failure is not easily recognized, so failure recovery is delayed, and there is a risk that a large-scale failure will affect many network users.

Therefore, NTT DOCOMO and Fujitsu, Ltd. jointly developed a system for rapid detection and identification of silent failures in IP networks [3]. That reduces the time to service restoration after a failure occurs, and can thus provide the user with safer, more secure, and more convenient services in the all-IP network NTT DOCOMO is building for the introduction of the LTE planned for December, 2010.

In this article, we present an overview of a silent failure detection system and briefly describe the "silent failure detection function" and "silent failure link identification function," which are the core functions of the system.

2. Conventional Silent Failure Detection Technology

One means of detecting silent failures is the connectivity monitoring system, which sends and receives test packets of mock telecommunication data called active probes to check connectivities. An overview is shown in **Figure 2**. This system sends active probes interspersed with communication packets over the telecommunication network that is being monitored. If a

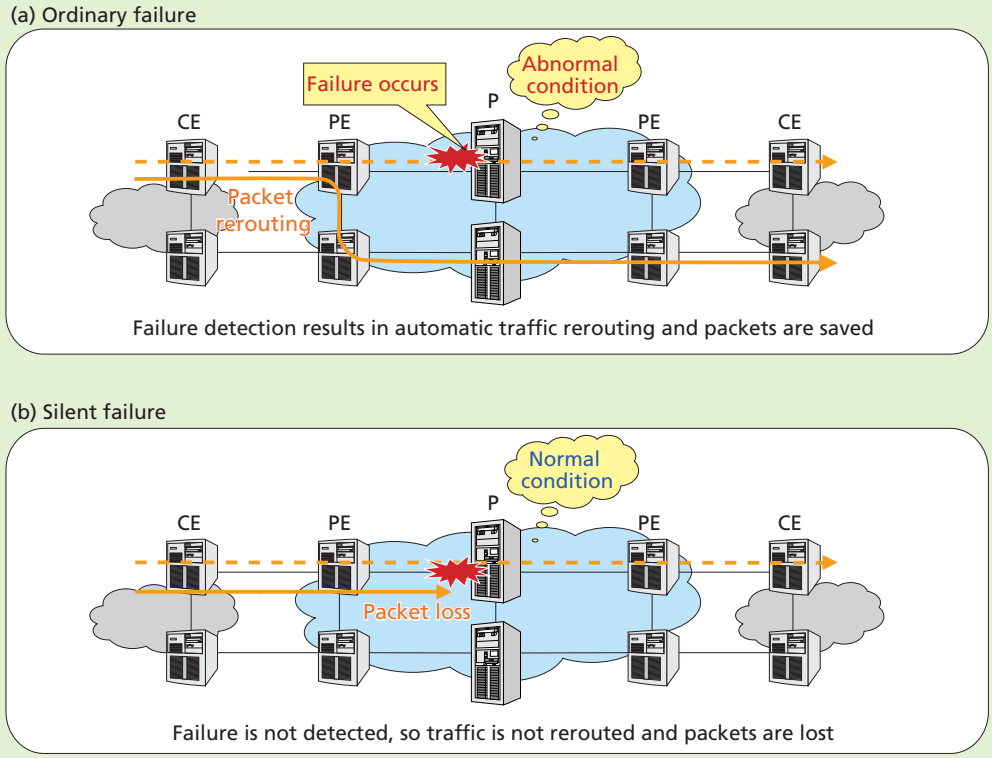

Figure 1 Effect of silent failure on an IP network

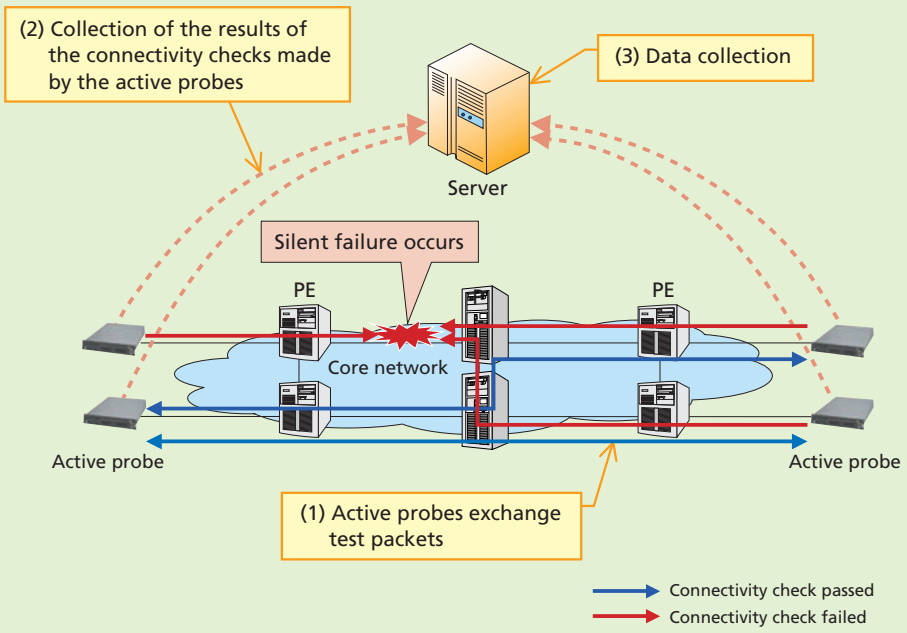

Figure 2 Overview of conventional connectivity monitoring system

communication problem arises, an alarm is issued. While this connectivity monitoring system can detect problems in communication between active probes, it cannot determine the cause of the problem. For that reason, no alarm is issued for connectivity problems that originate in failures that can be detected by conventional monitoring system as well as for silent failures, so maintenance personnel must check for alarms from both the conventional monitoring system and the connectivity monitoring system and reach an overall decision. At that time it is also necessary for the maintenance personnel to determine the path taken by the communication for which the connectivity problem arose between the active probes, and what equipment and alarms seem to be related to the connectivity problem.

The detection of silent failures with conventional monitoring systems and connectivity monitoring systems thus requires much time by maintenance personnel that have advanced technical abilities. Technology for distinguishing between ordinary failures and silent failures and rapid identification of the failure location in addition to simple detection is also needed.

3. Features of the Silent Failure Detection System

To overcome the issues of conventional technology, we developed a silent failure detection function and a silent failure link identification function. We also used those functions to construct a silent failure detection system to serve as a subsystem in an IP router network monitoring system. An overview of this silent failure detection system is shown in **Figure 3**.

3.1 Silent Failure Detection Function

The types of silent failure events include service disconnection and degradation of service quality, but the connectivity monitoring system described above targets only service disconnection. However, service quality degradation due to poor response caused by intermittent packet loss or other such factors also has the potential to disrupt service if it continues for a long period, so detection of such abnormal conditions is also important.

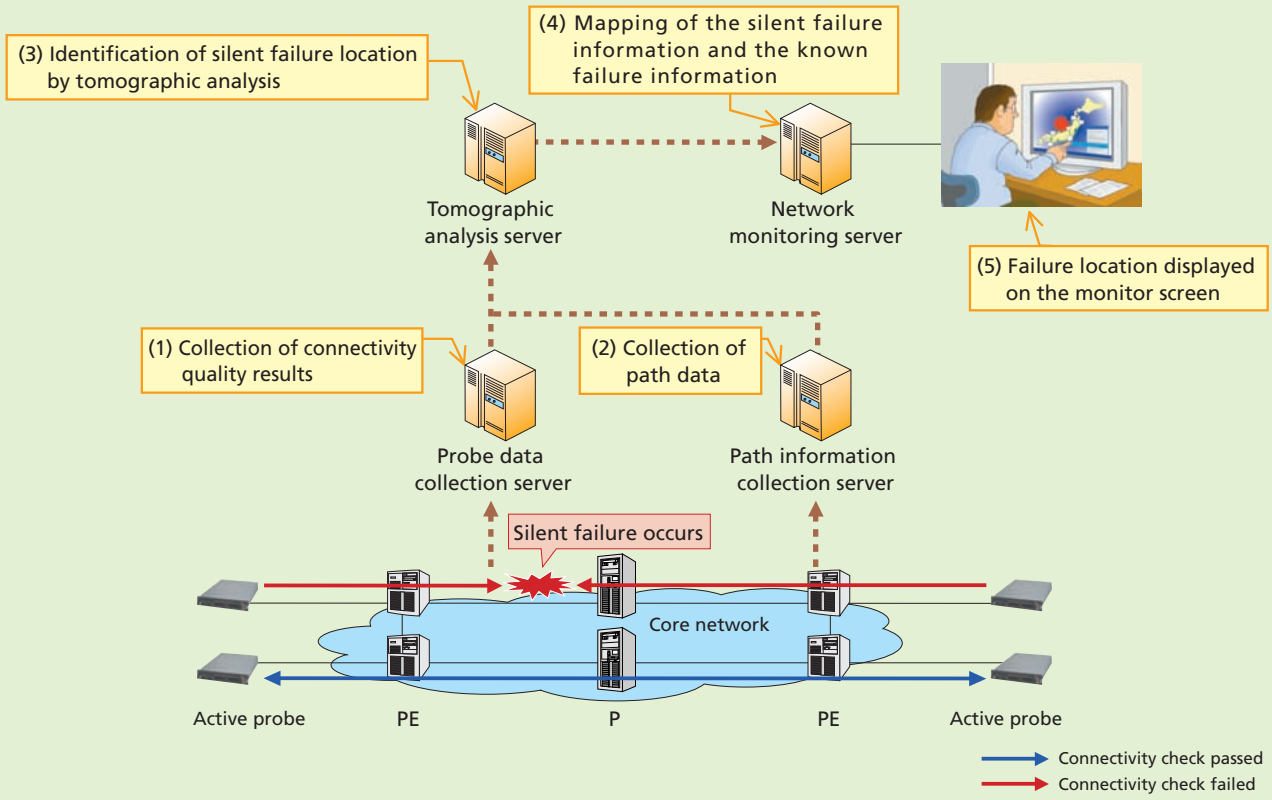

Figure 3 Overview of silent failure detection system

We therefore chose to have the silent failure detection function perform a packet loss rate and transmission delay quality check at the same time as the connectivity check. That makes it possible to understand both disconnection and quality degradation.

An overview of the silent failure detection function is shown in **Figure 4**. The probe collector and probe manager are higher-level servers that control the test packets on the sender-side (hereinafter referred to as "sender-side probes") and on the receiver-side (hereinafter referred to as "receiver-side probes"). The flow of processing is

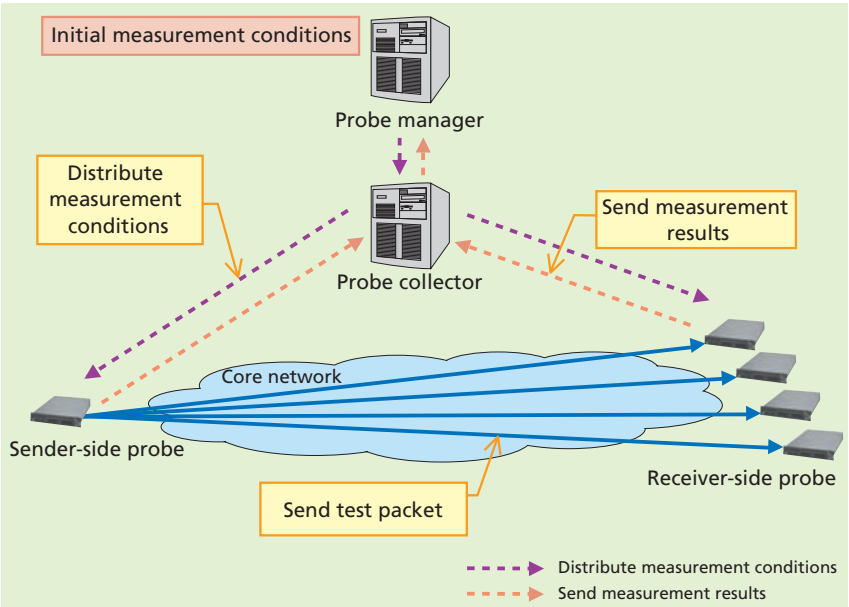

Figure 4 Overview of silent failure detection function

described below.

- The sender-side probe transmits test packets according to measurements such as the transmitted packet size and interval. The measurement conditions are made by the probe manager according to initial conditions and distributed by the probe collector.
- The receiver-side probe receives test packets from the sender-side probe.
- The test results from the sender-side probe (link end) and receiver-side probe (link end) are collected by the probe collector, and the probe manager determines the disconnection and quality degradation states between link ends.

Because the failures that are to be detected by this function include partial (particular end of a link) disconnection of communication only on a particular link as well as complete disconnection on a particular link (link connecting routers), a single sender-side probe regards all of the probes placed in the network (self probes excluded) as receiver-side probes and sends test packets to the receiving probes of all link ends.

3.2 Silent Failure Link Identification Function

The silent failure link identification function can rapidly identify the failure location by comprehensive analysis of the measurement results collected by the silent failure detection function, the path information generated by the path data retrieval function and the equipment status information that can be obtained from the conventional network monitoring function.

1) Path Data Retrieval Function

This function collects network path data and analyzes routing data to calculate inter-router path information. The generated path information is referenced by the tomography function that is described below and used to identify the failure location. The network that we target in this work uses the Open Shortest Path First (OSPF)[*4] routing protocol, and the path information collected is the OSPF Link-State Advertisement (LSA) information.

The path data is generated in the following way.

(1) Retrieve LSA data from routers specified in advance for each area of the OSPF network.
(2) Calculate the Shortest Path First (SPF) from the retrieved data.
(3) Generate a path between routers.

2) Tomographic Analysis Function

Tomographic analysis is used to rapidly determine the failure location on the basis of the measurement results obtained by the silent failure detection function and the path information generated by the path data retrieval function. An overview of the tomographic analysis function is shown in **Figure 5**.

Tomographic analysis generally refers to a way to visualize the internal structure of an object by making a number of cross sections, but here we use it to mean a method of determining the link in which a failure has occurred by overlaying connectivity quality measurement results and information on paths between routers. The tomographic analysis we use here was independently developed by Fujitsu Laboratories, Ltd. [4] and has the following features.

(1) The optimum solution is found simply by starting with a router to which an active probe is connected slicing the path on the basis of the connectivity relations of the upward and downward links and repeating the analysis for each router hop.
(2) Parallel processing and superimposition of the measurement results reduces the computation time in determining the failure location.
(3) A suspected location pattern in which failures occur in order of highest probability of occurrence can be derived.

Applying this method can reduce the computational cost of the analysis to about one-eighth, allowing high-speed failure detection.

3) Interworking with Conventional Network Monitoring Function

A failure in a link identified by the tomographic analysis function may

*4 **OSPF**: A routing protocol that selects the minimum cost path based on numerical data that indicates interface weighting values called cost.

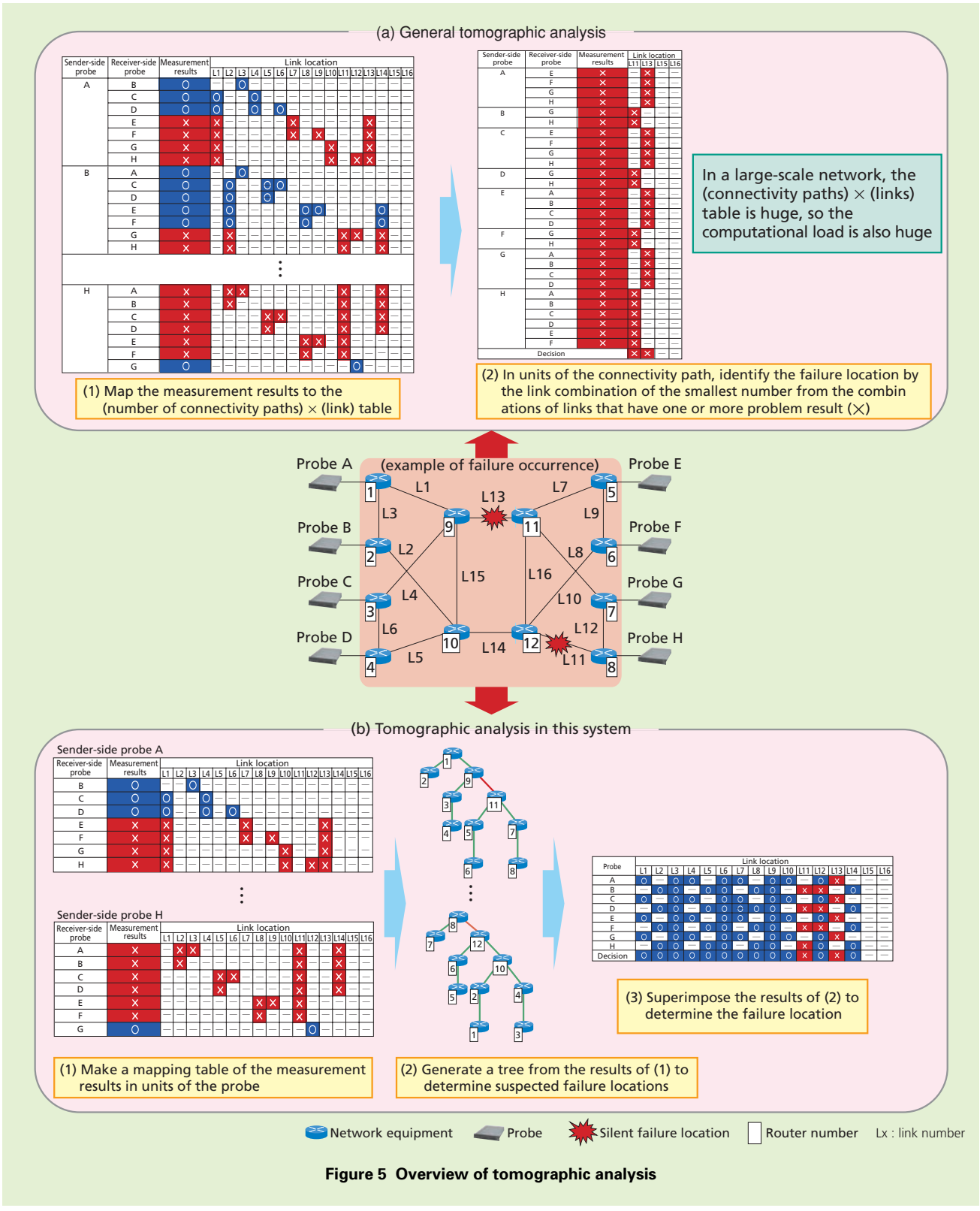

Figure 5 Overview of tomographic analysis

have already been detected by the conventional network monitoring function. Thus, cooperation of this function and the network monitoring function allows the minimum necessary failure information to be obtained by analyzing the correlations of the failures detected by the tomographic analysis function and the network monitoring function and that information can be made available to maintenance personnel.

4. Conclusion

In this article, we present an overview of a silent failure detection system for rapid and accurate detection of silent failures in an IP network and for determining failure location.

This system also implements functions for smooth operation of the telecommunication carrier network, such an automatic scenario distribution function for active probes at times of renovation or relocation of network equipment or the setting information entry support function. This system was introduced commercially in December, 2009 and is contributing to the stable operation of the IP router network.

In future work, we will continue with study of an automatic path rerouting function for when a silent failure is detected.

References

[1] Information and Communications Council, Issue No. 2020: "Measures for Data Communication network security and reliability (partial findings)," May 2007 (In Japanese).

[2] Information and Communications Council, Issue No. 2020: "Security and Reliability Standards for an All-IP Network," Jun. 2008 (In Japanese).

[3] NTT DOCOMO Press Release: "DOCOMO & Fujitsu Develop Counter-Failure Technologies for IP Networks," Dec. 2009.

[4] H. Matsuda, N. Fujinaka, J. Ogawa and T. Muramoto: "Proactnes II: Visualization for Next-Generation Network," FUJITSU, Vol.60, No.4, pp.387-392, Jul. 2009 (In Japanese).